International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Enhancing Organization Security using Attribute-Based Encryption for Data Sharing

Priya D. Tangde[1], A. S. Chhajed[2]

[1]M.E. Second Year, CSE,Anuradha Engineering College, Chikhli, Maharashtra, India

[2]Professor, Department of Information Technology, Anuradha Engineering College, Maharashtra, India

Abstract: ***The use of cloud computing technology is increasing rapidly and progressively. It provides various useful and essential services like data sharing, data storage .Organization can select services as per their requirement. While sharing of data in cloud security is an important aspect. Anyone can share their data in the cloud, but while sharing the data security is one of the challenging issues. The data can be protected from unauthorized person by encrypting it with proper key and should not able to access the private data. For this reason we need to take care of private data by implementing data protection techniques like cryptography. So as to make the data highly secured, the data are stored in encrypted format within the cloud. In this system our work is based on Attribute based Encryption. It is one of the techniques that are more suitable for storing data with encryption. The proposed scheme solves the key escrow problem. The proposed scheme solves the key escrow problem which dealt with key revocation mechanism. In the key revocation process of this system the user's key validity is removed. Paillier Cryptosystem is utilized for encryption of keys for assignment and revocation process while Twofish algorithm is used to encrypt and decrypt stored data of users.***

Keywords: Data Sharing, Attribute Based Encryption, Lucene, Paillier Cryptosystem

1. Introduction

To make confidentiality of data it should be in encrypted format. We provide access policy to share the data between users means based on that access policy user have the privilege to access the data. Cloud contains large amount of data stored in it, hence retrieving the correct information plays a very important role. Indexing can greatly improve the speed of information retrieval. The indexing of document collection is performed by Lucene. In the existing system KGC is not separated from master admin, hence master admin knows both keys that generated from KGC so in the absence of user master admin may access the private data. This problem is overcome in the proposed system as KGC is separated from the master admin.

Security is a most important thing in the data sharing. In the data sharing the main problem is leakage of data. The data can be protected by encrypting it with proper security key. In this system we have develop the data sharing using Attribute Based Encryption (ABE) Algorithm. By this our data becomes more secure than the existing system.

While sharing of data, the main objective is to provide Data confidentiality, Fine grained access control, Removing Key escrow problem, Removing Revocation problem, Scalability. The scope of this project is to protect the data from other persons in the network by encrypting it and send it in the social networks.

2. Existing Work

In Existing system the key pair that is private key & public key is generated using 2PC protocol. Encryption and Decryption of data is done with the help of both keys. The key escrow is the main problem in this system which is dealt with key revocation mechanism. The revocation mechanism contains the process of removing the private keys assigned to the user which is done by master admin. The key revocation doesn't fully resolved because only half key is revoke which is available in user whereas the private key still reside with the admin. In this system the KGC is not separated from master admin hence master admin knows both the keys so the private data may access by the master admin in the absence of user.

3. Literature Survey

Junbeom Hur [1] presents a novel CPABE scheme in which key escrow problem is solved by using key free issuing protocol using two way party computation protocol between KGC & Data storing center it generates & issues user secrete keys. They cannot fully trusted on KGC & data storing center, none of them could generate the whole set of users key alone. In this paper using proxy re-encryption with CPABE algorithm the immediate user revocation can be done. It enhances the backward / forward secrecy of data. The user revocation can be performed on each attribute level instead of system level for fine grained user access control. They also analyze & compare the efficiency of the proposed scheme with others CPABE schemes. The efficiency can be demonstrated in terms of computation cost for encrypting 7 decrypting a data. They present the computational cost in terms of table.

Apurva Gomase1,Prof. Vikrant Chole2 [2] in this paper they have done the servey on existing Attribute Based Encryption schemes & various approach with present their limitation and proposed novel CPABE scheme which is used to solve the key escrow problem by using escrow free key issuing protocol using two way party communications. They also provide proxy re encryption for fine grained user revocation for each attribute.

The comparative study of different ABE schemes like KP-ABE,CP-ABE, ABE with non monotonic access structure, HABE ,MABE have been present by Mangesh

Gosavi1,Tabassum Maktum2 [3] based on data confidentiality, fine grained access control, scalability, user revocation ,accountability &collusion resent and found that CPABE schemes for more efficient & scalable to manage the data in data sharing system.

There are two methods for access control based on ABE: Key-policy ABE (KP-ABE) and ciphertext-policy ABE (CPABE). Both notions are proposed in [4] by Goyal *et al.* In KP-ABE, each ciphertext is labeled with sets of attributes. Each attribute private key is associated with an access structure such that it can only decrypt a specific type of ciphertext. The first KP-ABE construction [4] can realize the monotonic access structures for key policies. To enable more flexible access policy, Ostrovsky *et al*. [5] presented the first KP-ABE system that supports the expression of non-monotone formulas in key policies. In a CP-ABE system, a user's key is associated with a set of attributes and an encrypted ciphertext will specify an access policy over attributes. CP-ABE is different from KP-ABE in the sense that the encryptor assigns certain access policy for the ciphertext. When a message is being encrypted, it will be associated with an access structure over a predefined set of attributes. Bethencourt *et al.* [5] proposed the first CP-ABE construction. However, the construction in [5] is only proved under the generic group model. In view of this weakness, Cheung and Newport [6] presented another construction that is proved to be secure under the standard model. Later, in [7], Goyal et al. gave another construction for more advanced access structures based on number theoretic assumption. To better protect user privacy, anonymous CPABE was constructed in [8] and further improved in [9]. Boneh and Waters [10] proposed a predicate encryption scheme based on the primitive called Hidden Vector Encryption. Their scheme can also realize the anonymous CP-ABE by using the opposite semantics of subset predicates. Recently, Katz, Sahai and Waters [11] proposed a novel predicate encryption scheme supporting inner product predicates and their scheme is very general and can realize both KP-ABE and hidden CP-ABE schemes.

4. Proposed System

In order to provide security and privacy in the proposed system it uses the concept of ABE encryption. This system provide the approach to enhance organization security for data sharing in cloud computing. It overcomes the drawback of existing system such as key escrow problem, key resolution & speed.

Advantages:

1) Data transfer with advanced encryption technique the unauthorized user cannot decrypt it easily.
2) Provide confidentiality & privacy of data in data sharing.
3) In the key revocation process of this system the users key validity is removed.

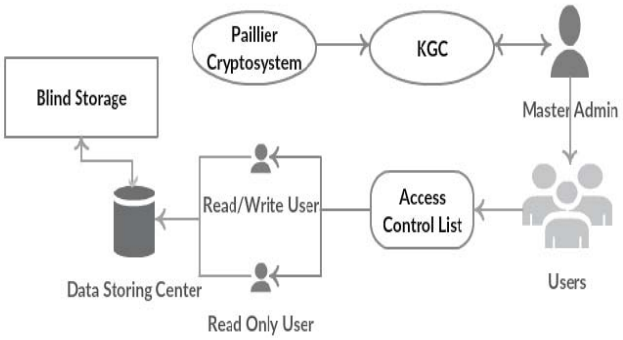


Figure 1: Proposed System Architecture

User Authentication

If new user wants to access the data for that he has to register first. In login module there are two fields username & password then it will be matched with database, if it is valid then that user will be granted to access the data, and if it is invalid then that user will be considered as unauthorized user & the access will be denied.

Key Generation center (KGC)

KGC has the authority to generate keys & stored in data storing center in encrypted form, which is not known to anyone since the KGC is not resides with the master admin.

Data Storaing Center

Data storing center is an entity which is used to store the data. When the user demands data from data storing center, blind storage methodology will ensure that data is fetched without disclosing any retrieval patterns. Whenever data owner upload personal documents on cloud server, first the keywords will get fetched from the documents and index will be created. For creating index of keywords fetched from document, Lucene indexing algorithm has been used. Lucene is full-text search engine architecture, provides: a complete query and indexing engine.

Paillier Cryptosystem

The Paillier Cryptosystem is a modular, public key encryption scheme, created by Pascal Paillier, with several interesting properties. This paper will explore Paillier's work[12], beginning by showing how to encrypt and decrypt messages using this cryptosystem, with the underlying mathematical principles that make the system work clearly outlined. It is assumed that the reader is familiar, to some degree, with modular arithmetic, as well as the concept of converting an alphanumeric message into a purely numeric message, which can be broken into blocks, mi, such that, for each i, $0 < mi < n$, for a predetermined value, n. Also, the term plaintext will be used to refer to a message that is numeric, but is not encrypted, while the term cipher text will be used to refer to plaintexts which have been encrypted, but not yet decrypted. Following an examination of the encryption and decryption process, several of the aforementioned interesting properties will be listed, and the math behind them explored. One property in particular, the addition of plaintexts through multiplication of cipher texts, will then be looked at in terms of its potential application to a form of electronic voting, in order to illustrate the system's potential[12].

In this paper, Paillier Cryptosystem is utilized for encryption of keys for assignment and revocation process while Twofish algorithm is used to encrypt and decrypt stored data of users.

Lucene Indexer

Apache Lucene is a free and open-source information retrieval software library, originally written in 100% pure Java by Doug Cutting. It is supported by the Apache Software Foundation and is released under the Apache Software License. Lucene's approach excelled at recommending documents with very similar structural characteristics and more narrow relatedness[13].

Whenever data owner upload personal documents on cloud server, it may have the security issues over the data confidentiality and authentication access control. The encryption technique used here is Twofish. Twofish is a symmetric key algorithm. It generates only one key which is a private key. When the key expires the user contacts with the master admin to generate a new key from KGC. The master admin generates the key and assigns the key to the user. If the user privileges are read and write the previously entered data is re-encrypted and is stored with the user.

Blind Storage

It supports only single keyword which will retrieve only small amount of file which will not satisfy the search user Dynamic Searchable Encryption via Blind Storage Muhammad Naveed, Manoj Prabhakaran[15] proposed a new storage scheme called Blind storage, which allows a client to store a set of files on a remote server in such a way that the server does not learn how many files are stored or the length of the individual file. Block cipher AES algorithm is used for encrypting and decrypting the file. To satisfy the client need single keyword search is implemented to retrieve the files related to the keyword. A new dynamic SSE scheme that is more efficient and simpler than prior schemes, achieving fully adaptive security.

Implementation Steps

Step 1: Registration of a user
Input: userid, password
Output: Registration Success
Step 2: Key Granting Center
Output: Generates random key for each user
Step 3: Paillier Encryption
Input: KGC generated Key
Output: Cipher Text
Step 4: Key Revocation
Output: Key Revocation Center revokes the key of user
Step 5: Key Update
Output: Key Update Center updates the key of user
Step 6: Storing User Service Information in Database
Input: Author name, Co-Authors, Paper Title, Technology used, Base Theory, Description
Output: Paper Uploaded Successfully
Step 7: XML to Database Parsing or Updation
Input: Insert SOA service adding data to XML files. Combine all data in the XML file.
Output: Database is updated.

Algorithm:-

Following flowchart represent Twofish algorithm

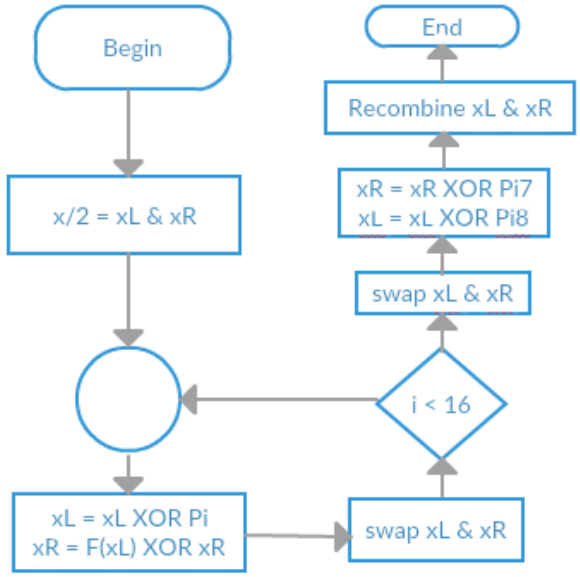


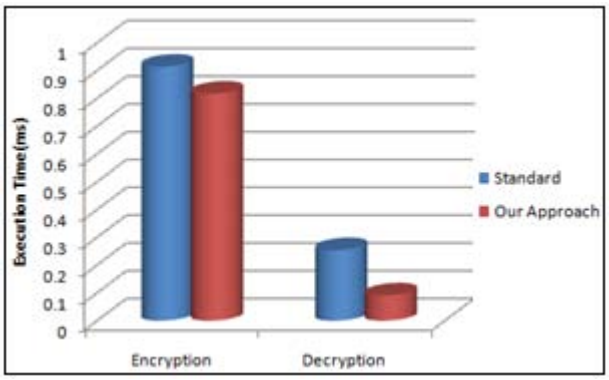
Figure 2: Flowchart of Twofish algorithm

(ii) The encryption of the data:
•64-bit input is denoted with an x
•P-array is denoted with a Pi (where i is the iteration).
•64-bit block size
•Key length - 32 bits to 448 bits (32-448 bits in steps of 8 bits; default 128 bits).
•16-round Feistel cipher
•Each line - 32 bits.

Algorithm keeps two sub-key arrays:
The 18-entry P-array
Four 256-entry S-boxes.
• S-boxes accept 8-bit input & produce 32-bit output.
• One entry of P-array is used every round.
•After final round, each half of data block is XORed with one of the two remaining unused P-entries.
•Initialize the P-array and S-boxes
• XOR subkey with plaintext.
o(example) P1 XOR (first 32 bits of key), P2 XOR (second 32 bits of key),
• New output of XL is apply to function .
• Output of function is XOR with XR bits
• Then perform swap operation.
• Repeat 16 times.

5. Performance Analysis

This section presents our evaluation results for encryption and decryption speed of existing and modified algorithm. Following Graph 1. represents the comparison of standard implementation & modified algorithm for encryption as well as decryption speed.



Graph 1: Graphical representation for both encryption & decryption speed of existing and modified algorithm

6. Conclusion

In this paper the proposed scheme issues a key that removes key escrow problem. Paillier Cryptosystem is utilized for encryption of keys for assignment and revocation process.In this proposed system modified algorithm take less speed for encryption and decryption as compared to existing algorithm. Thus this system achieves more secure and enhance organization security for data sharing in cloud computing.The resulting system effectively achieve confidentiality of documents and more secure than exiting system.

References

[1] Junbeom , "Improving Security and Efficiency in Attribute-Based Data Sharing", VOL. 25, NO. 10, OCT2013
[2] Apurva Gomase1,Prof. Vikrant Chole2,"A Review on Secure System Implementation using Attribute Based Encryption" IJCSMC, Vol. 3, Issue. 11, pg.465– 468, November 2014
[3] Mangesh Gosavi1,Tabassum Maktum2, "Survey of Various Attribute Based Encryption Schemes Used in Data Sharing System" IJARCSSE, 2015
[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
[5] Bethencourt J, Sahai A, Waters B," Ciphertext-policy attribute-based encryption. In: IEEE symposium on security and privacy". IEEE, Washington, DC, pp 321–334 2007
[6] Cheung L, Newport C "Provably secure ciphertext policy ABE. In: CCS" Proceedings of the 14th ACM conference on Computer and communications security. ACM, New York, pp 456–465,2007
[7] Goyal V, Jain A, Pandey O, Sahai A "Bounded ciphertext policy attribute based encryption." In: ICALP'08. LNCS 5126, pp 579–591 2008
[8] Kapadia A, Tsang PP, Smith SW "Attribute- based publishing with hidden credentials and hidden policies." In: Proc of network and distributed system security symposium (NDSS), pp 179–192,2007
[9] Li J, Kim "Attribute-based ring signature." Available at http://eprint.iacr.org/2008/394,2008
[10] Boneh D, Waters B,"Conjunctive, subset, and range queries on encrypted data." In: TCC'07. LNCS 4392. Springer, pg 535–554,2007
[11] Katz J, Sahai A, Waters B, "Predicate encryption supporting disjunctions, polynomial equations, and inner products." In: EUROCRYPT'08. LNCS 4965. Springer, New York, pg 146–162, 2008
[12] Michael O'Keeffe, "The Paillier Cryptosystem" The College of New Jersey Mathematics Department April 18, 2008
[13] Addagada, Sridevi, "Indexing and Searching Document Collections using Lucene" University of New Orleans Theses and Dissertations. Paper 1070,2007
[14] Shucheng Yu , Cong Wang , Kui Ren, "Attribute Based Data Sharing with Attribute Revocation:" Proc. ACM Symp. Information,Computer and Comm. Security (ASIACCS '10), 2010.
[15] Muhammad Naveed, Manoj Prabhakaran, Carl A. "Dynamic Searchable Encryption via Blind Storage" Gunter University of Illinois at Urbana-Champaign 2014
[16] A. Lewko, A. Sahai, and B. Waters, "Revocation Systems with Very Small Private Keys," Proc. IEEE Symp. Security and Privacy, pg 273-285, 2010.
[17] D. Kavitha, S. Hemavathy, "A Survey on Cloud Computing Security Issues And Multi-Keyword Ranked Data Search Efficiency in Blind Storage" Vol. 3, Issue 9, September 2015
[18] Keerthi B, V Rajesh kannan, "Implementation of Attribute Hiding Strategy and Key Revocation in Cloud Environment" IJISET Vol. 1 Issue 2, April 2014.
[19] A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf.Computer and Comm. Security, pp. 195-203, 2007.
[20] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-Based Systems", Proc. ACM Conf. Computer and Comm. Security, 2006
[21] Bheri Thrinadha1, Ramesh kumarBehara2, "Provide Privacy and Efficiency of Multi Authority Data Access Control Over Cloud Computing" International Journal of Engineering Trends and Technology (IJETT) – Volume 30 Number 5 - December 2015